UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/634,117 | 08/04/2003 | James M. Doherty | 1033-T00534 | 5753 |

84326 7590 08/05/2009

AT & T LEGAL DEPARTMENT - Toler
ATTN: PATENT DOCKETING
ROOM 2A-207
ONE AT & T WAY
BEDMINISTER, NJ 07921

| EXAMINER | |
|---|---|
| HOANG, DANIEL L | |
| **ART UNIT** | **PAPER NUMBER** |
| 2436 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 08/05/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

---

*Ex parte* JAMES M. DOHERTY, THOMAS LEE ADAMS, and STEPHEN MARK MUELLER

---

Appeal 2008-004072
Application 10/634,117
Technology Center 2400

---

Decided: August 5, 2009

---

*Before* JAMES D. THOMAS, HOWARD B. BLANKENSHIP, and DEBRA K. STEPHENS, *Administrative Patent Judges*.

STEPHENS, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134 from a final rejection of claims 1, 3-15, and 17-27. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

*Introduction*

According to Appellants, the invention is directed to a system and method for detecting intrusions to a host computer system interfaced to a computer network (Abstract).

*Exemplary Claim(s)*

Claims 1, 14, and 15 are exemplary claims and are reproduced below:

1. A method comprising:

providing a host computer system having at least one network interface interfaced with a computer network;

operating the host computer system in a multi-user mode;

detecting an intrusion event using a system daemon; and

in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

14. A method comprising:

providing a host computer system having at least one network interface interfaced with a computer network;

operating the host computer system in a multi-user

mode;

executing a system daemon on the host computer system;

reading, by the system daemon, a configuration me that indicates at least one file in a file system of the host computer system to be monitored for intrusion, wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion;

reading a valid MD5 signature for a monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system;

detecting an intrusion event using the system daemon by detecting that an MD5 signature of the monitored file differs from the valid MD5 signature; and

in response to detecting the intrusion event:

issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network;

issuing an lNlTl command to an operating system of the host computer system to take the host computer system down to a single user state;

and

writing a log of the intrusion event to a log database that is not located on the second computer system.

15. A system comprising:

a host computer system having at least one network interface interfaced with a computer network, the host computer system to:

operate in a multi-user mode;

detect an intrusion event using a system daemon; and

in response to detecting the intrusion event, isolate the at least one network interface from the computer network and take the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

*Prior Art*

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

| | | |
|---|---|---|
| Mann | US 6,081,894 | Jun. 27, 2000 |
| Douglas | US 2004/0049693 A1 | Mar. 11, 2004 |

*Rejections*

The Examiner rejected claims 1, 3-15, and 17-27 under 35 U.S.C. § 103(a) as being unpatentable over Douglas and Mann. [1]

GROUPING OF CLAIMS

Appellants have grouped claims together to address the grounds of rejection (App. Br.4-9, § VII.). We consider Appellants' groupings which group the claims together as follows:

(1) Claims 1, 3 and 5-13 as a group in response to the rejection under 35 U.S.C. § 103(a) based on Appellants' arguments regarding claim 1. We will, therefore, treat dependent claims 3 and 5-13 as falling with representative independent claim 1.

(2) Claim 4 independently in response to the rejection under 35 U.S.C. § 103(a).

(3) Claims 15 and 17-27 as a group in response to the rejection under 35 U.S.C. § 103(a) based on Appellants' arguments regarding claim

---

[1] Claims 2 and 16 have been cancelled by Appellants in their RESPONSE TO NON-FINAL OFFICE ACTION received September 12, 2006. Although both Appellants and the Examiner have in places mistakenly referred to the outstanding claims as including cancelled claims 2 and/or 16, we note Appellants specifically indicate claims 1, 3-15, and 17-27 are on appeal and claims 2 and 16 have been cancelled (App. Br. 1, § III, subsec. A. – C. and Reply Br. 1, § I, subsec. A. – C.). Additionally, the Examiner responded to arguments regarding only the outstanding claims 1, 3-15, and 17-27 (Ans. 6-9, § (10), subsec. I and II). Therefore, we conclude claims 2 and 16 have been cancelled and claims 1, 3-15, and 17-27 are the claims on appeal.

15. We will, therefore, treat claims 17-27 as falling with representative independent claim 15.

(4) Claim 14 independently based on the rejection under 35 U.S.C. § 103(a).

*See* 37 C.F.R. § 41.37(c)(1)(vii) ("Notwithstanding any other provision of this paragraph, the failure of appellant to separately argue claims which appellant has grouped together shall constitute a waiver of any argument that the Board must consider the patentability of any grouped claim separately.").

## ISSUES

*Issue 1: 35 U.S.C. § 103(a): claims 1, 3, 5-13, 15, and 17-27*

*Appellants' Contentions*

Appellants assert their invention is not obvious over Douglas and Mann (App. Br. 4, § VII). Specifically, Appellants contend neither Douglas nor Mann teach that "in response to detecting an intrusion event, isolating at least one network interface from a computer network and taking a host system down to a single user state so that access to the host computer system is limited to physical access at the host computer system" as recited in claim 1 (*Id.*). Appellants further argue Mann discloses that the data sending entity is isolated from the data receiving entity without disrupting normal operation of either entity – which is different than taking the system down to a single

user state (App. Br. 4-5, § VII). Since neither the "data isolator" nor the "data receiving entity" of Mann are in a multi-user state, it is unclear how the data sending entity could ever be reduced to a single user state without disruption of normal operation (*Id.*).

*Examiner's Findings*

The Examiner finds Mann teaches the normal operation of either entity is not disrupted when isolation occurs (Ans. 6, § (10), subsec. I)). The Examiner further finds Mann teaches the data receiving entity is a personal computer or local area network and thus is the host computer system; the data sending entity is the Internet; and communication between the personal computer and the Internet is operating in multi-user mode (*Id.*). The Examiner then finds isolating the computer from the Internet results in the computer operating in a single user state (*Id.*).

*Issue 1:* Have Appellants met the burden of showing the Examiner erred in finding Mann teaches that when an intrusion is detected, the host system is taken down to a single user state so that access to the host computer system is limited to physical access at the host computer system?

*Issue 2: 35 U.S.C. § 103(a): claims 4 and 14*

*Appellants' Contentions*

Appellants contend Mann does not disclose or suggest that, to the extent isolation is disclosed, the isolation is achieved by activating a data isolator and not by issuing commands to a host computer system (App. Br. 6, § VII).

*Examiner's Findings*

The Examiner finds Mann teaches that, when a virus is detected, a control line from the processor causes the power up control logic circuit to cause the power supply conditioning ISO drive to shut off power to the optical isolator – which takes the host computer system down to a single user state (Ans. 8, § (10), subsec. II).

*Issue 2:* Have Appellants met the burden of showing the Examiner erred in finding Mann teaches issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to the single user state?

FINDINGS OF FACT (FF)

*Appellants' Invention*

(1) A host system comprises one or more computers accessible via a computer network, such as a server computer, a corporate mainframe computer, and a desktop computer (Spec. 2, [1009]). A computer network may be an Internet, an extranet, a local area network, or a wide area network (*Id.*).

(2) Typically, the normal operating mode of the host system 10 is a multi-user state wherein multiple users can access the host system 10 via the computer network 12 (Spec. 4, [1019]; Fig. 1).

(3) If no intrusion event is detected, the host system 10 continues in its normal operating mode allowing external access via network interfaces 14 (Spec. 4, [1019]; Fig. 1; Fig. 2, block 46). If an intrusion event is detected, the system daemon generates an alarm (Spec. 4, [1020]; Fig. 1; Fig. 2, block 46). The host system performs acts to protect the rest of the computer network including issuing commands to isolate the host system from the computer network (Spec. 4, [1021]; Fig. 1; Fig. 2, blocks 46, 54, and 56).

*Mann's Invention*

(4) Mann teaches an apparatus and method for isolating a data receiving entity from a data sending entity when a virus or similar data is detected (Abstract).

(5) A data receiving entity such as a personal computer or local area network, receives and evaluates data received from a data sending entity such as the Internet (col. 2, ll. 61-64).

(6) When a virus or other data is detected, a data isolator, responsive to a control signal, isolates the data receiving entity from the data sending entity and thus viruses are prevented from being received by the data receiving entity (col. 1, ll. 15-18; col. 1, ll. 38-41; col. 2, ll. 45-48; col. 3, ll. 2-7). The data sending entity is physically isolated from the data receiving entity upon detecting a data virus without disrupting normal operation of either entity (col. 2, ll. 30-32; claim 12).

## PRINCIPLES OF LAW

### *Claim Construction*

"The Patent and Trademark Office (PTO) must consider all claim limitations when determining patentability of an invention over the prior art." *In re Lowry*, 32 F.3d 1579, 1582 (Fed. Cir. 1994) (citing *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983)). "Claims must be read in view of the specification, of which they are a part." *Markman v. Westview Instruments, Inc.,* 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc) (citations omitted).

### *Obviousness*

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

"What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under *§ 103*." *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 419 (2007). To be nonobvious, an improvement must be "more than the predictable use of prior art elements according to their established functions." *Id.* at 417.

ANALYSIS

*35 U.S.C. § 103(a): claims 1, 3, 5-13, 15, and 17-27*

Both Appellants and Mann have a host system – Appellants state the host system may be a computer accessible via a computer network such as a desktop computer; Mann states the data receiving entity (host system) may be a personal computer or local area network (FF 1 and FF 4). Thus, both Appellants and Mann disclose a computer connected to a computer network and both disclose the computer network may be the Internet (FF 1 and FF 5).

Appellants argue that Mann does not teach the host computer is in a multi-user mode and thus may not be taken down to a single user mode (App. Br. 5, § VII). Multi-user mode is not defined by Appellants. Taking the broadest reasonable interpretation consistent with the Specification, Appellants disclose the host system may be a single computer connected to the Internet – which Mann also teaches (FF 1 and FF 4). Thus, we find the host system connected to the Internet is operating in a multi-user mode as various users could be accessing the host system (e.g., to place an order with a book seller).

Additionally, the Examiner relies on Douglas to teach this feature (Ans. 3). Appellants' arguments focus on the individual differences between the limitations of claim 1 and the Mann reference. It is apparent, however, from the Examiner's line of reasoning in the Final Rejection, that the basis for the obviousness rejection is the combination of Douglas and Mann. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. *In re Keller*, 642 F. 2d 413, 425 (CCPA 1981); *In re Merck & Co., Inc.*, 800 F. 2d 1091, 1096 (Fed.

Cir. 1986). In other words, while Appellants contend that Mann lacks a teaching, it is our view that such feature is taught by Douglas for the reasons set forth by the Examiner.

Appellants further argue Mann does not teach taking the host computer system down to a single user state (App. Br. 4-5, §VII.). Appellants do not define single user state; however, taking the broadest reasonable interpretation consistent with the Specification, we find Mann discloses this feature (FF 6). Indeed, both Appellants and Mann physically isolate the host system from the computer network when an intrusion is detected (FF 3 and FF 6). Mann additionally teaches when the personal computer (host system) is isolated from the computer network, the personal computer still operates normally, but due to the isolation, access may only be acquired to the host system locally, not through the Internet (FF 6). Therefore, we find Mann teaches, when an intrusion event is detected, the host computer system is taken down to a single user state – e.g., the host computer cannot be used by other users on the Internet.

Appellants next argue the "single user state" is a different state from normal operation and taking the host system down to a single user state disrupts normal operation (App. Br. 5, §VII.). This argument is unpersuasive in convincing us the Examiner erred. Instead, we find the "normal operation" taught by Mann is that the host system (data receiving entity) and the computer network (data sending entity) may continue to function even though the entities have been isolated. "A further advantage of the invention is that it isolates the data sending entity from the data

receiving entity without disrupting normal operation of either entity" (col. 2, ll. 30-32).

Additionally, Appellants' arguments that since Mann teaches other embodiments (i.e., the data sending entity is a local area network), it does not teach the present invention (Reply Br. 7) is unpersuasive.

Accordingly, we find Mann teaches when an intrusion is detected, the two computer systems are isolated from each other. We additionally find Mann teaches when the isolation occurs, the host computer operates normally in a single user state.

Therefore, we conclude Appellants have not met the burden of showing the Examiner erred in finding Mann teaches, when an intrusion is detected, the host system is taken down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

*35 U.S.C. § 103(a): claims 4 and 14*

The Examiner finds that Mann teaches, when a virus is detected, a control line from the processor causes the power up control logic circuit to cause the power supply conditioning ISO drive to cut off power to the optical isolator, thereby, causing the optical isolator to prevent passage of data (Ans. 8, § (10), subsec. I.). Appellants have not presented any arguments to overcome the Examiner's finding.

Appellants additionally argue the Examiner has not pointed out the particular bases for the rejection of claim 14 (App. Br. 8, § VII.). The Examiner set forth the bases for the rejection of claim 14 as applied to

claims 1-8 and 10. Claims 1-8 and 10 recite analogous language or the same language for every limitation of claim 14, except "executing a system daemon on the host computer system." However, we find that in mapping claim 4, the Examiner mapped this limitation.

Accordingly, we conclude Appellants have not met the burden of showing the Examiner erred in finding Mann teaches issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to the single user state.

*Additional Issues*

Lastly, we find Appellants' Response to Examiner's Argument (Reply 5-7) provides very little rebuttal to the Examiner's Answer. Instead, we find Appellants present several new arguments related to the combinability of the references including alleged use of hindsight, use of mere conclusory statements, and teaching away by the cited prior art. None of these new arguments were presented in the first instance in the Appeal Brief and thus will not be addressed by us.

Therefore, based on the record before us, it is our view Appellants have not met the burden of showing the Examiner erred in finding modifying the system of Douglas with the technique of Mann would be obvious to one skilled in the art. Therefore, we find the combination of Douglas and Mann teaches or suggests the argued limitations of "taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system" (*see* independent claim 1 and analogous language recited in each of

independent claims 14 and 15). Accordingly, Appellants have not shown that the Examiner has erred.

We affirm the Examiner's rejection of independent claims 1, 14, and 15 and dependent claim 4 as being obvious over Douglas and Mann. Since claims 3-13 depend from independent claim 1 and claims 3 and 5-13 were not argued separately, claims 3 and 5-13 fall with independent claim 1. Additionally, since claims 17-27 depend from independent claim 15 and claims 17-27 were not argued separately, claims 17-27 fall with claim 15.

## CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude Appellants have not met the burden of showing the Examiner erred in finding Mann teaches that, when an intrusion is detected, the host system is taken down to a single user state so that access to the host computer system is limited to physical access at the host computer system. Moreover, Appellants have not met the burden of showing the Examiner erred in finding Mann teaches issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to the single user state. Accordingly, Appellants have not met the burden of showing the Examiner erred in rejecting claims 1, 3-15, and 17-27 under 35 U.S.C. § 103(a) for obviousness over Douglas and Mann.

.

DECISION

The Examiner's rejection of claims 1, 3-15, and 17-27 under 35 U.S.C. § 103(a) as being obvious over Douglas and Mann is affirmed.

AFFIRMED

PEB

AT & T LEGAL DEPARTMENT - Toler
ATTN: PATENT DOCKETING
ROOM 2A-207
ONE AT & T WAY
BEDMINISTER, NJ 07921